Journal of Number Theory **73**, 527–532 (1998)
Article No. NT982285

A Note on the Irreducibility of Hecke Polynomials

Kevin James and Ken Ono*

Department of Mathematics, Pennsylvania State University, University Park, Pennsylvania 16802
E-mail: klj@math.psu.edu and ono@math.psu.edu

Communicated by A. Hildebrand

Received February 23, 1998; revised April 17, 1998

Let S_{2k} denote the space of modular cups forms of weight $2k$ for $SL_2(\mathbb{Z})$. If $f(z) := \sum^{\infty}$. $a_f(n)\, q^n \in S_{2k}$ (here $q := e^{2\pi i z}$ throughout), and p is prime.

$$T_p^{2k} f := \sum_{n=1}^{\infty} \left(a_f(np) + p^{2k-1} a_f(n/p)\right) q^n.$$

Let $T_p^{2k}(x)$ denote the characteristic polynomial of the action of T_p^{2k} on S_{2k}. It is well known that $T_p^{2k}(x) \in \mathbb{Z}[x]$ and has degree d_k where $d_k := \dim(S_{2k})$. However, much more is conjectured to be true. Maeda has conjectured that the Hecke algebra of S_{2k} over $\mathbb{Q}$ is simple, and that its Galois closure over $\mathbb{Q}$ has Galois group S_{d_k}. Recently there have been numerous investigations regarding the irreducibility of characteristic polynomials of Hecke operators on S_{2k}. The existence of such polynomials have proven to be useful in proving nonvanishing theorems for central values of level 1 modular L-functions, and in constructing base changes to totally real number fields for level 1 eigenforms (see [C-F, H-M, Ko-Z]).

In this note we show that a "positive proportion" of the Hecke polynomials $T_p^{2k}(x)$ are irreducible if there are two distinct primes ℓ and q for which $T_q^{2k}(x)$ is irreducible over $\mathbb{F}_\ell$, the finite field with ℓ elements. Throughout p will denote a prime number.

THEOREM 1. *If there are distinct primes ℓ and q for which the Hecke polynomial $T_q^{2k}(x)$ is irreducible in $\mathbb{F}_\ell[x]$, then*

$$\#\{p < X \mid T_p^{2k}(x) \text{ is irreducible in } \mathbb{Q}[x]\} \gg_k \frac{X}{\log X}.$$

* The second author is supported by NSF Grant DMS-9508976 and NSA Grant MSPR-97Y012.

0022-314X/98 $25.00

This result follows immediately from the following more general result.

As usual, we will let $S_k(N, \chi)$ denote the space of modular cusp forms of weight k, level N and character χ. For $f(z) = \sum_{n=1}^{\infty} a_f(n)\, q^n \in S_k(N, \chi)$ and $p \nmid N$ the Hecke operator $T_{N,p}^{k,\chi}$ is defined by

$$T_{N,p}^{k,\chi} f = \sum_{n \geq 1} (a_f(np) + \chi(p)\, p^{k-1} a_f(n/p))\, q^n.$$

Let $T_{N,p}^{k,\chi}(x)$ denote the characteristic polynomial of $T_{N,p}^{k,\chi}$ on $S_k^{\text{new}}(N, \chi)$. Moreover, let $\mathbb{K}_{k,\chi,N}$ denote the finite extension of $\mathbb{Q}$ obtained by adjoining the roots of all of the $T_{N,p}^{k,\chi}(x)$ with $p \nmid N$.

THEOREM 2. *Let q and ℓ be distinct primes not dividing N, and let $\mathscr{L}$ denote a prime ideal of $\mathbb{K}_{k,\chi,N}$ lying above ℓ. Then*

$$\#\{p < X \mid T_{N,p}^{k,\chi}(x) \equiv T_{N,q}^{k,\chi}(x) \pmod{\mathscr{L}}\} \gg_{N,\chi,k} \frac{X}{\log X}.$$

Proof. Let $\{f_1, ..., f_d\}$ be a basis of $S_k^{\text{new}}(N, \chi)$ such that each f_i is an eigenform for all of the $T_{N,p}^{k,\chi}$ where $p \nmid N$. Let $\lambda_{f_i}(p)$ be the eigenvalue of $T_{N,p}^{k,\chi}$ corresponding to the eigenform f_i (i.e. $T_{N,p}^{k,\chi} f_i = \lambda_{f_i}(p)\, f_i$). By the work of Deligne, Serre and Shimura [D, D–S, Sh], there exist continuous representations

$$\rho_{f_i,\mathscr{L}} : \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \text{GL}_2(\mathscr{O}_{\mathscr{L}})$$

satisfying the following conditions:

(i) $\rho_{f_i,\mathscr{L}}$ is unramified for $p \nmid N\ell$,

(ii) $\text{trace}(\rho_{f_i,\mathscr{L}}(\text{Frob}_p)) = \lambda_{f_i}(p)$ for $p \nmid N\ell$,

(iii) $\det(\rho_{f_i,\mathscr{L}}(\text{Frob}_p)) = \chi(p)\, p^{k-1}$ for $p \nmid N\ell$.

Here $\mathscr{O}$ denotes the ring of integers of $K_{k,\chi,N}$, $\mathscr{O}_{\mathscr{L}}$ denotes its completion at $\mathscr{L}$ and Frob_p denotes any Frobenius element for p. Let $\mathfrak{l}$ denote a uniformizer for $\mathscr{O}_{\mathscr{L}}$. By reducing the representations $\rho_{f_i,\mathscr{L}}$ modulo $\mathfrak{l}$, we obtain representations from $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ to $\text{GL}_2(\mathscr{O}_{\mathscr{L}}/\langle \mathfrak{l} \rangle)$. These representations have finite image and therefore factor to yield representations:

$$\bar{\rho}_{f_i,\mathscr{L}} : \text{Gal}(K/\mathbb{Q}) \to \text{GL}_2(\mathscr{O}_{\mathscr{L}}/\langle \mathfrak{l} \rangle),$$

where K is a finite extension of $\mathbb{Q}$.

By the Chebotarev density theorem, there is a set S of rational primes having positive Dirichlet density and having the property that for each

$p \in S$, $\mathrm{Frob}_{\mathfrak{P}}$ is conjugate to $\mathrm{Frob}_{\mathfrak{Q}}$, where $\mathfrak{P}$ and $\mathfrak{Q}$ are prime ideals of K lying above p and q respectively, and therefore have the property that for each $1 \leqslant i \leqslant d$

$$\mathrm{trace}(\bar{\rho}_{f_i, \mathscr{L}}(\mathrm{Frob}_{\mathfrak{P}})) \equiv \lambda_{f_i}(p) \pmod{\mathrm{l}} \qquad \text{if} \quad p \nmid N\ell.$$

Since the trace is conjugation invariant, it follows that for $p \in S$,

$$\lambda_{f_i}(p) \equiv \lambda_{f_i}(q) \pmod{\mathrm{l}}.$$

Since the $\lambda_{f_i}(p)$ $(1 \leqslant i \leqslant d)$ are precisely the roots of $T_{N,p}^{k,\chi}(x)$, the theorem follows. ∎

EXAMPLE. Here we shall give a simple example that illustrates Theorem 2. We consider the Hecke polynomials on the three dimensional space $S_5^{\mathrm{new}}(11, \chi_{-11})$. For convenience, let $T_p(x)$ denote the characteristic polynomial for the Hecke operator $T_{11,p}^{5,\chi_{-11}}$. The first few terms of the Fourier expansions of the three newforms are

$$\begin{aligned}
N_1(z) &= \sum_{n=1}^{\infty} a_1(n)\, q^n \\
&= q + 7q^3 + 16q^4 - 49q^5 - 32q^9 + \cdots, \\
N_2(z) &= \sum_{n=1}^{\infty} a_2(n)\, q^n \\
&= q + \sqrt{-30}\, q^2 - 3q^3 - 14q^4 + 31q^5 \\
&\quad - 3\sqrt{-30}\, q^6 - 10\sqrt{-30}\, q^7 + \cdots, \\
N_3(z) &= \sum_{n=1}^{\infty} a_3(n)\, q^n \\
&= q - \sqrt{-30}\, q^2 - 3q^3 - 14q^4 + 31q^5 \\
&\quad + 3\sqrt{-30}\, q^6 + 10\sqrt{-30}\, q^7 - \cdots.
\end{aligned}$$

It is easy to verify that if $p \neq 11$ is prime, then

$$a_2(p) = a_3(p) \in \mathbb{Z} \qquad \text{if} \quad \left(\frac{p}{11}\right) = 1 \tag{1}$$

and

$$a_2(p) = -a_3(p) \qquad \text{if} \quad \left(\frac{p}{11}\right) = -1. \tag{2}$$

Moreover, if $(\frac{p}{11}) = -1$, then

$$\frac{a_2(p)}{\sqrt{-30}} \in \mathbb{Z}. \tag{3}$$

These all follow from standard facts about eigenvalues of Hecke operators (e.g. [Kob]).

The form $N_1(z)$ has complex multiplication by $\mathbb{Q}(\sqrt{-11})$ in the sense of Ribet (see [R]). By construction, there is exactly one such form in this space. In particular if $p \neq 11$ is prime, then

$$a_1(p) = \begin{cases} 0 & \text{if} \quad \left(\frac{p}{11}\right) = -1, \\ \dfrac{2x^4 - 132x^2y^2 + 242y^4}{16} & \text{if} \quad \left(\frac{p}{11}\right) = 1 \quad \text{and} \quad 4p = x^2 + 11y^2. \end{cases}$$

This implies that if $p \neq 11$ is prime, then

$$a_1(p) \equiv \begin{cases} 0 \pmod{11} & \text{if} \quad \left(\frac{p}{11}\right) = -1, \\ 2p^2 \pmod{11} & \text{if} \quad \left(\frac{p}{11}\right) = 1. \end{cases} \tag{4}$$

Now if $B(z) = \sum_{n=1}^{\infty} b(n)\, q^n$ is defined by

$$\begin{aligned} B(z) &:= \frac{15 + \sqrt{-30}}{30} \cdot N_2(z) + \frac{15 - \sqrt{-30}}{30} \cdot N_3(z) \\ &= q - 2q^2 - 3q^3 - \cdots, \end{aligned}$$

then the methods of Swinnerton-Dyer [S-D] suggest that $B(z)$ may satisfy a congruence with a linear combination of twisted Eisenstein series. Using a theorem of Sturm [St], we verify indeed that there is such a congruence modulo 11, and it turns out that

$$b(n) \equiv \left(8n + 4n\left(\frac{n}{11}\right)\right) \sum_{d \mid n} d^7 \pmod{11}. \tag{5}$$

By combining (1–5), if $p \neq 11$ is prime, then

$$T_p(x) \equiv \begin{cases} x^3 + 5x^2 + x + 3 \pmod{11} & \text{if } p \equiv 1 \pmod{11}, \\ x^3 + 8x \pmod{11} & \text{if } p \equiv 2 \pmod{11}, \\ x^3 + 10x^2 + 3 \pmod{11} & \text{if } p \equiv 3 \pmod{11}, \\ x^3 + 8x^2 + 4 \pmod{11} & \text{if } p \equiv 4 \pmod{11}, \\ x^3 + 9x^2 + 2x + 9 \pmod{11} & \text{if } p \equiv 5 \pmod{11}, \\ x^3 + 10x \pmod{11} & \text{if } p \equiv 6 \pmod{11}, \\ x^3 + 8x \pmod{11} & \text{if } p \equiv 7 \pmod{11}, \\ x^3 + 7x \pmod{11} & \text{if } p \equiv 8 \pmod{11}, \\ x^3 + x^2 + 6x + 3 \pmod{11} & \text{if } p \equiv 9 \pmod{11}, \\ x^3 \pmod{11} & \text{if } p \equiv 10 \pmod{11}. \end{cases}$$

If p is a prime for which $(\frac{p}{11}) = 1$, then by (1) and (4) we see that $T_p(x)$ factors into three linear factors in $\mathbb{Z}[x]$. If p is a prime for which $(\frac{p}{11}) = -1$ and $a_2(p) \neq 0$, then by (2) and (3) it follows that $T_p(x)$ factors into irreducibles in $\mathbb{Z}[x]$ as

$$T_p(x) = x(x^2 + a_2(p)^2).$$

By (5) one easily finds that $a_2(p) \neq 0$ for every such $p \equiv 2, 6, 7, 8 \pmod{11}$.

REFERENCES

[B] K. Buzzard, On the eigenvalues of the Hecke operator T_2, *J. Number Theory* **57** (1996), 130–132.

[C-F] B. Conrey and D. Farmer, Hecke operators and the nonvanishing of L-functions, preprint.

[D] P. Deligne, Formes modulaires et représentations ℓ-adiques, *Sem. Bourbaki* **355** (1969),.

[D-S] P. Deligne and J.-P. Serre, Formes modulaires de poids 1, *Ann. Sci. École Norm. Sup. (4)* **7** (1974).

[H-M] H. Hida and Y. Maeda, Non-abelian base change for totally real fields, *Pacific J. Math.*, in press.

[Kob] N. Koblitz, "Elliptic Curves and Modular Forms," Springer-Verlag, Berlin, 1984.

[Ko-Z] W. Kohnen and D. Zagier, Values of L-series of modular forms at the center of the critical strip, *Invent. Math* **64** (1981), 175–198.

[R] K. Ribet, Galois representations attached to eigenforms with Nebentypus, *in* "Modular Functions of One Variable V," Lecture Notes in Math., Vol. 601, pp. 17–51, Springer-Verlag, Berlin, 1977.

[Sh] G. Shimura, "Introduction to the Arithmetic Theory of automorphic Functions," Iwanami Shoten and Princeton Univ. Press, Tokyo/Princeton, NJ, 1971.

[St] J. Sturm, On the congruence of modular forms, *in* "Lecture Notes in Math.," Vol. 1240, pp. 275–280, Springer-Verlag, New York/Berlin, 1987.

[S-D] H. P. F. Swinnerton-Dyer, On ℓ-adic representations and congruences for coefficients of modular forms, *in* "Modular Functions of One Variable III," Lecture Notes in Math., Vol. 350, pp. 1–55, Springer-Verlag, New York/Berlin, 1973.